UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,084	03/26/2001	Michael E. Graves	12307/100173	2846

23838 7590 08/01/2006

KENYON & KENYON LLP
1500 K STREET N.W.
SUITE 700
WASHINGTON, DC 20005

EXAMINER	
WORJLOH, JALATEE	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 08/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/818,084
Filing Date: March 26, 2001
Appellant(s): GRAVES ET AL.

David J. Zibelli (Registration No. 36,394)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 05/24/2006 appealing from the Office action mailed 07/26/2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6205437	Gifford	3-2001
2001/0044787	Shwartz et al.	11-2001
2004/0243520	Bishop et al.	12-2004
2001/0014158	Baltzley	8-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 35, 37-42,44-49, 51-55 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6205437 to Gifford in view of U.S. Publication NO. 2004/0243520 to Bishop et al. and US Publication NO. 2001/0044787 to Shwartz et al.

Referring to claims 35 and 42, Gifford discloses storing a public key associated with a public key infrastructure (PKI) key pair in a profile database (see col. 10, lines 37-42), in response to receiving an authentication request from a buyer over a network, the authentication request including a description of the payment transaction and an identity of a seller (see col. 6,

lines 16-32), storing a digitally signed record of the payment transaction in a transaction archive, i.e. "transaction database" (see col. 8, lines 16-19) and sending an authentication response to the seller over the network (see col. 6, lines 52-61). Gifford does not expressly disclose sending a challenge request to the buyer over the network, the challenge request including a summary of the payment transaction to be displayed to the buyer and then digitally signed by the buyer using a private key associate with the PKI key pair, or in response to receiving a challenge response from the buyer over the network, the challenge response including the digitally singed summary of the payment transaction, determining whether the buyer has access to the private key by using the public key to decrypt the digitally signed message. Bishop et al. disclose sending a challenge request to the buyer over the network, the challenge request message to be displayed to the buyer then digitally signed by the buyer using a private key associate with the PKI key pair, or in response to receiving a challenge response from the buyer over the network, the challenge response including the digitally singed message, determining whether the buyer has access to the private key by using the public key to decrypt the digitally signed message (see paragraphs [0094] & [0095]). Shwartz et al. disclose the challenge request including a summary of the payment transaction (see paragraphs [0182]-[0184]). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Gifford to include the steps of sending a challenge request to the buyer over the network, the challenge request including a summary of the payment transaction to be displayed to the buyer and then digitally signed by the buyer using a private key associate with the PKI key pair, or in response to receiving a challenge response from the buyer over the network, the challenge response including the digitally singed summary of the payment transaction, determining

whether the buyer has access to the private key by using the public key to decrypt the digitally signed message. One of ordinary skill in the art would have been motivated to do this because it protects the network server from attacks and improve the ease and safety of electronic commerce for consumers (see Bishop et al. & Shwartz et al.).

Referring to claims 37,44 and 51, Gifford discloses the method wherein the record of the payment transaction is digitally signed using the private key (see col. 10, lines 43-45).

Referring to claims 38,45 and 52, Gifford discloses the method wherein the record of the online transaction is digitally signed using a local private key (see col. 10, lines 48 & 49).

Referring to claims 39,46 and 53, Gifford discloses the method wherein the public key is stored in the form of a digital certificate representing that the public key is tied to the buyer (see col. 7, lines 44-46).

Referring to claims 40,47 and 54, Gifford discloses several databases including account database storing account information and an address database storing shipping address information (see col. 8, lines 12-24 and 33-36). Gifford also discloses receiving a selection of one of the plurality of payment instruments (i.e. "means of payment") and one of the plurality of shipping addresses from the buyer over the network (see col. 5, lines 34-50; col. 8, lines 33-35). Gifford does not expressly disclose retrieving a buyer profile from the database, the buyer profile including a plurality of payment instruments and a plurality of shipping address and sending the buyer profile to the buyer over the network; however, these are inherent steps. Before selecting the method of payment and address information, the buyer must first be provided with his profile.

Referring to claims 41,48 and 55, Gifford discloses processing the payment transaction via a payment gateway (i.e. "payment computer") see col. 6, lines 12-14.

Referring to claim 49, Gifford discloses a profile database, i.e. account database and address database, transaction archive, i.e. settlement database" (see col. 7, lines 66-67 & col. 8, lines 1-7) an authentication service web server (i.e. "payment computer") coupled to the profile database, the transaction archive and the network, the authentication service web server adaptively configured to (see col. 4, lines 46-55) store a public key associated with a public key infrastructure (PKI) key pair in a profile database (see col. 10, lines 37-42), in response to receiving an authentication request from a buyer over a network, the authentication request including a description of the payment transaction and an identity of a seller (see col. 6, lines 16-32), store a digitally signed record of the payment transaction in a transaction archive, i.e. "transaction database" (see col. 8, lines 16-19) and send an authentication response to the seller over the network (see col. 6, lines 52-61). Gifford does not expressly disclose the web server adaptively configured to send a challenge request to the buyer over the network, the challenge request including a summary of the payment transaction to be displayed to the buyer then digitally signed by the buyer using a private key associate with the PKI key pair, or in response to receiving a challenge response from the buyer over the network, the challenge response including the digitally singed summary of the payment transaction, determine whether the buyer has access to the private key by using the public key to decrypt the digitally signed summary of the payment transaction. Bishop et al. disclose sending a challenge request to the buyer over the network, the challenge request message to be displayed to the buyer then digitally signed by the buyer using a private key associate with the PKI key pair, or in response to receiving a challenge

response from the buyer over the network, the challenge response including the digitally singed message, determining whether the buyer has access to the private key by using the public key to decrypt the digitally signed message (see paragraphs [0094] & [0095]). Shwartz et al. disclose the challenge request including a summary of the payment transaction (see paragraphs [0182]-[0184]). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Gifford to include the steps of the web server adaptively configured to send a challenge request to the buyer over the network, the challenge request including a summary of the payment transaction to be displayed to the buyer then digitally signed by the buyer using a private key associate with the PKI key pair, or in response to receiving a challenge response from the buyer over the network, the challenge response including the digitally singed summary of the payment transaction, determine whether the buyer has access to the private key by using the public key to decrypt the digitally signed summary of the payment transaction. One of ordinary skill in the art would have been motivated to do this because it protects the network server from attacks and improve the ease and safety of electronic commerce for consumers (see Bishop et al. & Shwartz et al.).

3. Claims 36,43 and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gifford, Bishop et al. and Shwartz et al. as applied to claims 35, 42 and 49 above, and further in view of US Publication NO. 2001/0014158 to Baltzley.

Gifford discloses PKI key pair (see claims 35 and 42 above). Gifford does not expressly disclose creating the PKI key pair, and sending the private key to the buyer over the network. Baltzley discloses creating the PKI key pair (see paragraph [0010], and sending the private key

to the buyer over the network (see paragraph [0011]). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Gifford to include the steps of creating the PKI key pair, and sending the private key to the buyer over the network. One of ordinary skill in the art would have been motivated to do this because it prevents fraud by providing additional security.

(10) Response to Argument

Appellants present arguments regarding Davis and Barnett references; however, these references were not relied upon in the Final Rejection. Thus, all arguments regarding Davis and Barnett are moot.

Appellants argue that "The express purpose of the challenge response in Bishop is to solve the problem of replay attacks, which was already solved by the invention of Gifford" and that "the nonce used in Gifford already protects against replay attacks so that one of ordinary skill in the art would not have been motivated to add the challenge and response of Bishop to solve the replay attacks problem already solved by the nonce of Gifford." Notice, whether or not the problem was previously solved is irrelevant. If, as asserted by Appellants, the problem was already solved, it only provides additional support that Appellants' limitations are obvious.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir.

1992). In this case, the prior art utilized are analogous and all recognizes the need for security in electronic payment systems. Specifically, Gifford states that there is a need in credit card payment system to reduce the risk of fraud.

Citation from col. 2, lines 22-34:

> In existing credit card payment systems, a credit card's issuing bank takes on the fraud risk associated with misuse of the card when a merchant follows established card acceptance protocols. Acceptance protocols can include verifying a card holder's signature on the back of their card and obtaining authorization for payments over a certain value. However, in network based commerce a merchant can not physically examine a purchasers credit card, and thus the fraud risk may revert to the merchant in so called "card not present" transactions. Many merchants can not qualify to take this risk because of their limited financial resources. Thus the invention is important to allow many merchants to participate in network based commerce.

Bishop et al. also emphasizes the need to improve security deficiencies of payment transactions.

Citation from paragraph [0006]:

> To improve the security deficiencies inherent in transporting charge card numbers over unsecure networks, many have suggested the use of "smart cards". Smart cards typically include an integrated circuit chip having a microprocessor and memory for storing data directly on the card. The data can correspond to a cryptographic key, for example, or to an electronic purse that maintains an electronic value of currency. Many smartcard schemes have been suggested in the prior art, but these typically exhibit a marked disadvantage in that they are non-standard. In other words, merchants typically must obtain new, proprietary software for their Web storefronts to accept smartcard transactions. Moreover, the administration costs involved with assigning and maintaining the cryptographic information associated with smart cards have been excessive to date.

Finally, Shwartz et al. also states that it is necessary to "improve the ease and safety of electronic commerce for consumers" (see paragraph [0014]).

Appellants argue that "there is no suggestion that a component of the challenge message is to be displayed to the user and then digitally signed by the buyer" in Bishop et al. reference; however, the Examiner respectfully disagrees. Notice, Bishop et al. teach receiving a challenge message and forwarding the challenge data to a browser as signature request message. Later, a smartcard suitably signs the block. It is known in the art that browsers are utilized to view documents; thus, the data of Bishop et al. is forwarded to the browser, which implies that the document will be displayed and later signed.

Appellants argue that Shwartz et al. fail to teach "the challenge request including a summary of the payment transaction to be displayed to the buyer and then digitally signed by the buyer". The *challenge request including a summary of the payment transaction* is given the broadest reasonable interpretation. Therefore, as recited in paragraph [0183], "the front-end client presents a window on the display of the communication device asking approval for the transaction and presenting the challenge"; "asking approval for transaction" is inherently providing *a summary of the payment transaction.* That is, it is known in the art of payment authorization that when a user is asked for a confirmation he is provided with a summary of the purchase order including the purchase item, price, date and total cost. Thus, with the broadest reasonable interpretation it is clear that Shwartz et al. teaches this feature.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

JW

Conferees:

Sam Sough
Appeal Conference Specialist
Superviosry Primary Examiner
Art Unit 3628

James Reagan
Primary Examiner
Art Unit 3621